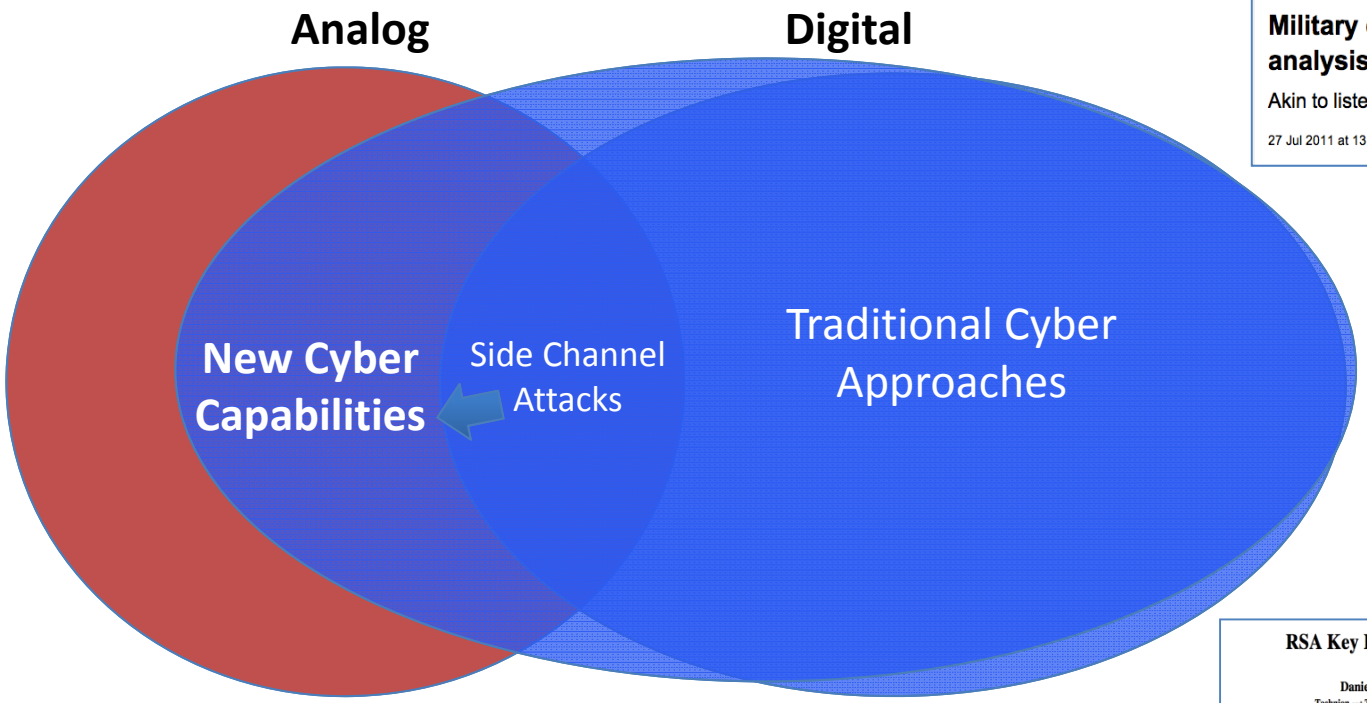
Leveraging the Analog Domain for Security

Angelos D. Keromytis
Program Manager
Information Innovation Office (I2O)

October 1, 2015

Unexplored Opportunities for Cybersecurity at the Intersection of Analog and Digital



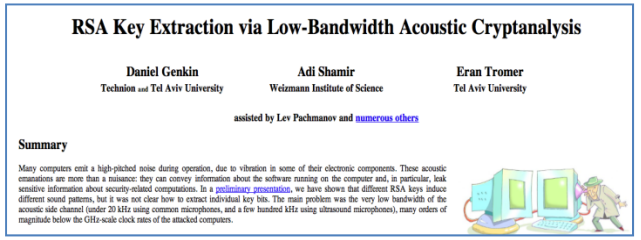

The Register
Biting the hand that feeds IT

DATA CENTER SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES

Military chip crypto cracked with power-analysis probe

Akin to listening to safe tumblers, but with 'leccy

27 Jul 2011 at 13:54, John Leyden 117 17 23


RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

Daniel Genkin, Technion and Tel Aviv University
Adi Shamir, Weizmann Institute of Science
Eran Tromer, Tel Aviv University

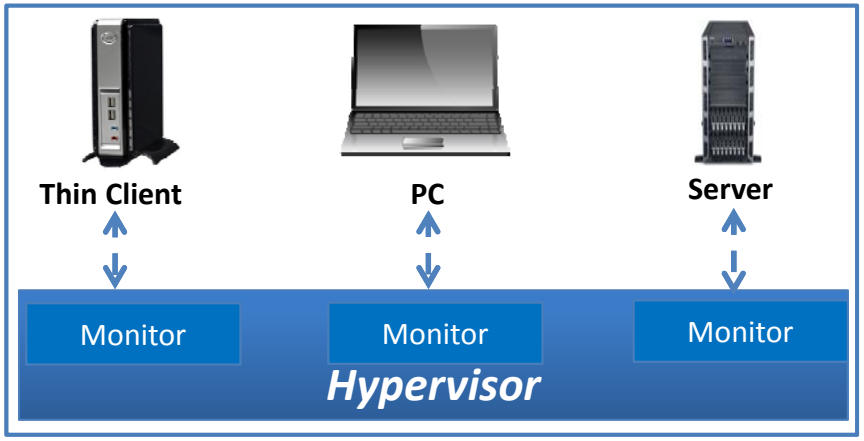
assisted by Lev Pachmanov and numerous others

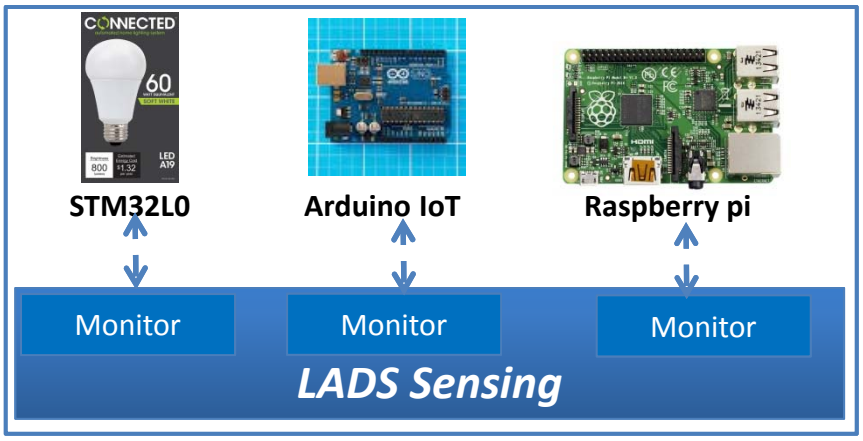
Summary

Many computers emit a high-pitched noise during operation, due to vibration in some of their electronic components. These acoustic emanations are more than a nuisance: they can convey information about the software running on the computer and, in particular, leak sensitive information about security-related computations. In a preliminary presentation, we have shown that different RSA keys induce different sound patterns, but it was not clear how to extract individual key bits. The main problem was the very low bandwidth of the acoustic side channel (under 20 kHz using common microphones, and a few hundred kHz using ultrasound microphones), many orders of magnitude below the GHz-scale clock rates of the attacked computers.

- Analog and digital are generally viewed as distinct areas in cybersecurity
  - Ignoring the analog side simplifies an already hard problem
  - We can usually afford to rely only on digital techniques (i.e., more code/logic)

Using Analog to Protect Low-Resource Devices





Traditional IT:

- Resource-rich environment with numerous existing and new capabilities for cyber defense
- Defenses do not readily translate to low-resource environments

IoT and Embedded:

- Resource, logistic, and physical constraints make it difficult to embed security functionality
- Attack surface is large and easy to exploit
- Single penetration leads to total compromise


NETWORKWORLD Most read:

Researchers exploit ZigBee security flaws that compromise security of smart homes

Network World | Aug 11, 2015 10:54 AM PT


The Register

Security

Compromised Cisco routers spotted bimbling about in the wild

Diseased boxen lassoed in four countries as malicious actors find their way into systems


SECURELIST

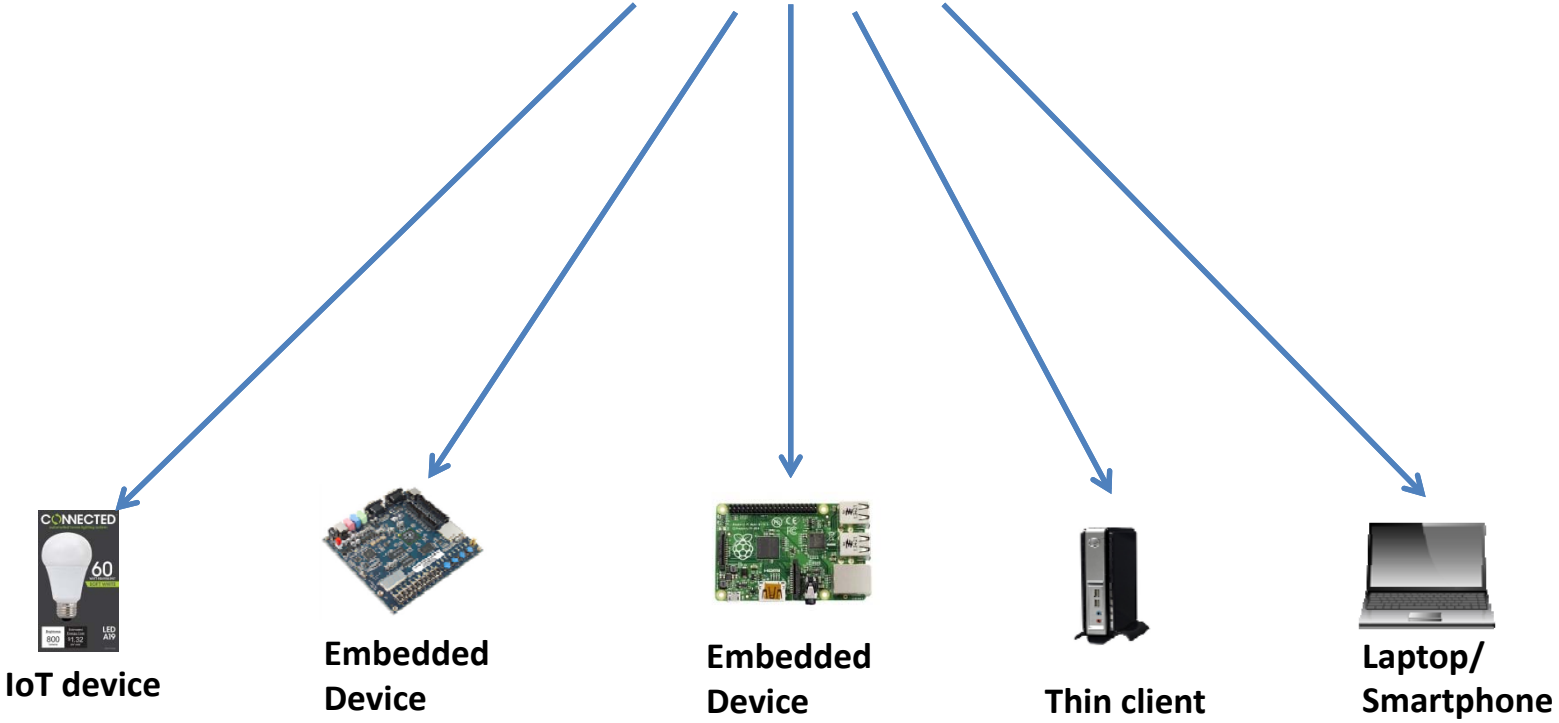
Equation: The Death Star of Malware Galaxy

By GReAT on February 16, 2015. 6:55 pm

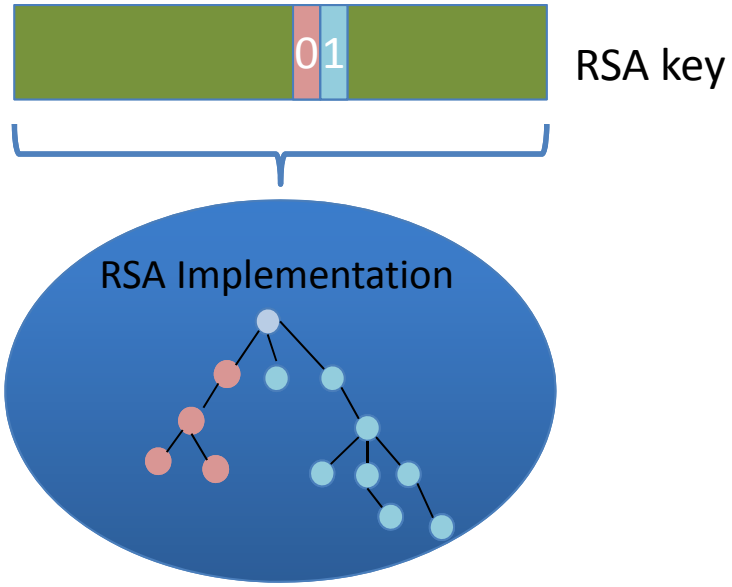
Use the analog domain to enable new classes of defense in low-resource and embedded devices (e.g., IoT)

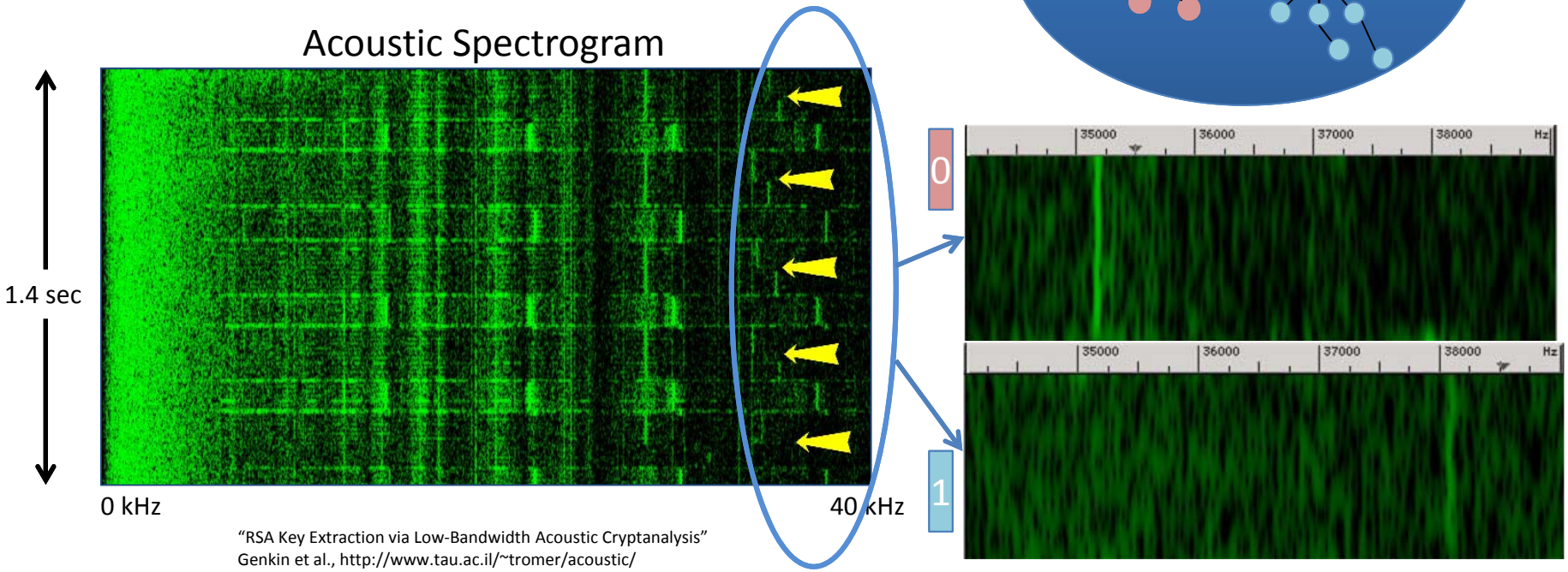
LADS Program Structure

TA1: Protecting Embedded and Mission-Specific Devices (EMSDs) via Analog Sensing



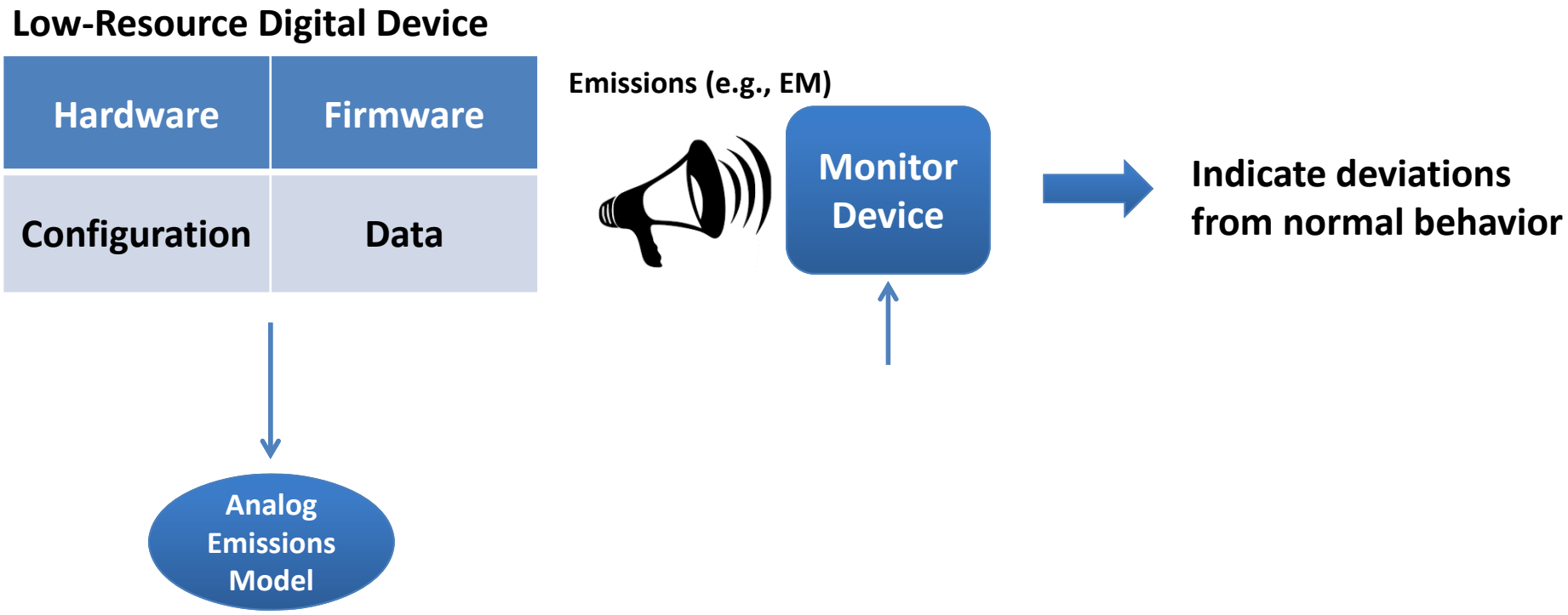
Example: Extract Cryptographic Keys by Tracking Code Execution Acoustically





"RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"
Genkin et al., http://www.tau.ac.il/~tromer/acoustic/

LADS: Protecting EMSDs via Analog Sensing



- Explore different emission modalities
  - e.g., EM, acoustic, power
- Combine multiple modalities
- Many-to-one, many-to-many tracking

LADS Program Structure

TA1: Protecting Embedded and Mission-Specific Devices (EMSDs) via Analog Sensing

- ***Goal:*** Develop new cyber techniques in digital devices by monitoring the analog emissions across different/multiple modalities:
  - Tracking fidelity vs. device complexity
  - Fidelity: Known/unknown code, control flow tracking, instruction tracking, …

Parameters/Challenges:
- **Distance**
- **Polarization**
- **Multipath**
- **Ambient Noise**

- ***Output*****:** Monitoring devices; network architectures; algorithms for mapping digital artifacts to analog emissions

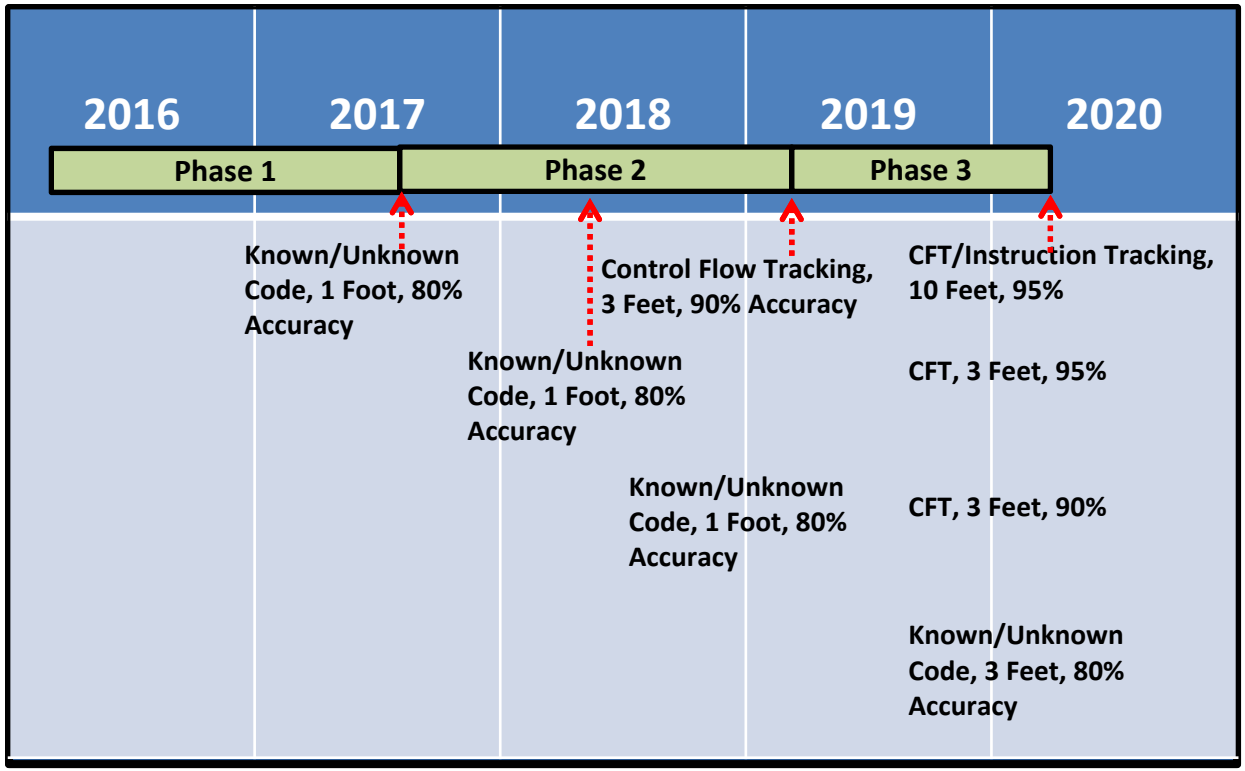
- ***Methodology:***
  - Identify and quantify useful analog signals
    - Develop predictive models
  - Map device firmware, configuration, and data to cyber-relevant analog emissions model
    - Unknown firmware & configuration
  - Boost signal via software and/or analog component modifications
- Reconcile tracked device emissions with emissions model
- Cooperative sensing and tracking

TA1 Program Metrics

- Measure effectiveness as a ROC curve (detection vs. misdetection) on devices of increasing complexity
  - Fidelity: Known/unknown code, control flow tracking, instruction tracking, others
  - Secondary characteristics depending on modality, e.g., distance, polarization
- Phase 1 Program Metrics:
  - Demonstrate feasibility of discriminating between known/unknown code executing on a simple IoT-type device
    - 80% accuracy or higher, assuming knowledge of the firmware
    - Close proximity (signal level of 3dBi or less at 1 foot), in an environment with low ambient noise (Demonstration at Month 18)
  - Demonstrate the impact of modifying the software executing on the device to boost detection of software/firmware compromise
- Phase 2 Program Metrics:
  - Demonstrate the ability to correctly identify with 80% accuracy, at close proximity (1 foot), from among several instances of known code/unknown code, while improving accuracy (90%) and distance (3 feet or more) for the simpler devices
    - FPGA board by M30, thin-client computer or simple “feature phone” cell phone by M36
    - Demonstrate the techniques for devices of increasing complexity
- Phase 3 Program Metrics:
  - Extend the techniques for more complex devices (e.g., a high-end smartphone or laptop) while increasing accuracy, fidelity, and discriminating capability for the devices examined in earlier phases
    - Improve accuracy to 95% with close proximity to 10 feet (Demonstration at M48)

Program Schedule and Progress Metrics

Primary Metrics:
- **Fidelity**
- **Distance**
- **Accuracy**



Evaluation Details

- Each performer conducts own evaluation for each milestone
  - Provide data and prototypes to DARPA and AFRL to conduct independent validation
  - Government reserves the right to engage third parties to independently validate results

- Each performer responsible for specifying in their proposal which devices they will use, for each of the four device classes
  - Make your choices based on proposed sensing modalities
  - Avoid selection of Government-/DoD-specific equipment
  - Suggestion: Specify groups of devices in each class
    - Government may choose to limit to a subset, or propose substitute devices during contract negotiations

Meetings and Reporting Requirements

- Two Annual Principal Investigator (PI) Meetings
- Quarterly Technical Reviews between PI Meetings
- Monthly Progress Reports
  - Technical Report describing progress, resources expended and issues requiring Government attention, provided 10 days after the end of each month
- Financial/Technical Progress Reporting to the DARPA Technology Financial Information Management System (TFIMS)
- Software Development Plan
- Final Technical Report
- Agent: AFRL/RYMH

Funding and Programmatic Details

- Proposals due: Tuesday, November 17 at noon ET
- Government anticipates multiple awards
  - Procurement Contract or Other Transaction
- Proposers to TA1 are not required to hold or obtain security clearances
- Proposers to TA1 do not require access to the LADS Classified Addendum
- Organizations can submit separate proposals to all Technical Areas
  - Which to consider for award is at the discretion of the Government
- To expedite award contracting, proposers are encouraged to have sub-award agreements in place ahead of award notification

Leveraging the Analog Domain for Security (LADS) Program DARPA-BAA-15-61

Mark Jones

DARPA Contracts Management Office

Proposers Day
Arlington, VA
October 1, 2015

DISCLAIMER

If the BAA contradicts any information in these slides,

the BAA takes precedence.

BAA OVERVIEW

- BAA follows procedures in accordance with FAR 35.016.
- BAA is posted on FEDBIZOPPS at www.fbo.gov (as well as any future amendments).
- Proposals due by 12:00 noon ET on November 17, 2015
- BAA covers all info needed to submit proposals. Follow instructions for proposal preparation and submittal.

POTENTIAL AWARD INFORMATION

- One Unclassified Technical Area (TA)
- Anticipate multiple awards – exact award numbers or amounts have not been predetermined
- Program structured in 3 phases – Base and 2 Options
- Awards may be Procurement Contracts or Other Transaction Agreements (OTs). No grants or Cooperative Agreements will be awarded.

BAA ELIGIBILITY

- All interested/qualified sources may respond subject to the parameters outlined in the BAA.

- Foreign organization/individuals – check all applicable Security Regulations, Export Control Laws, Non-Disclosure Agreements, and any applicable governing statutes.

- FFRDCs and Government entities
  - Subject to applicable direct competition limitations
  - Must clearly demonstrate eligibility per BAA

- Real and/or Perceived Conflicts of Interest
  - Identify any conflict
  - Include mitigation plan

- Classified Portion eligibility addressed in BAA Addendum

PROPOSAL PREPARATION INFORMATION

- Proposals consist of two volumes – Technical and Cost.

- Volume 1 - Technical and Management
  - Volume 1 has maximum 30 page limit
  - Includes mandatory Appendix A – does not count towards page limit.
  - Includes optional Appendix B – does not count towards page limit
  - Includes optional Appendix C – does count towards page limit

- Volume 2 – Cost - No page limit.

- The BAA will describe the necessary information to address in each volume –
  - Make sure to include every section identified.
  - If a section does not apply – put “None” (e.g., Animal Use – None, OCI - None)
  - Include a working/unprotected spreadsheet as part of your Cost Volume submission.
  - Review individual TA descriptions, IP and the deliverables section for submittal information

PROPOSAL PREPARATION TIPS

- **Statement of Work (SOW)** – Write a SOW as if it were an attachment to a contract
  - Don't use proposal language (e.g. we propose to do . . .)
  - Break out work between any phases/time periods identified in the BAA
  - Succinctly and clearly define tasks & subtasks
  - Do not include any proprietary information!

- **Risk** – Do not be afraid to address Risk in Technical Volume
  - Identify risk(s) to show an understanding of technical challenge(s)
  - Discuss potential mitigation plans / alternative directions

PROPOSAL PREP – INTELLECTUAL PROPERTY RIGHTS

- Government desires, at a minimum, **Government Purpose Rights** for any proposed noncommercial software and technical data. (SEE DFARS 227 for Patent, Data, and Copyrights)

- Since LADS will emphasize creating and leveraging open architecture technology, IP rights and software licenses asserted by proposers are strongly encouraged to be aligned with this goal.

- Data Rights Assertions – IF asserting **less than Unlimited Rights**:
  - Provide and justify basis of assertions
  - Explain how the Government will be able to reach its program goals (including transition) within the proprietary model offered; and
  - Provide possible nonproprietary alternatives

- IF proposed solution utilizes commercial IP – submit copies of license with proposal

ITEMS TO NOTE

- Work expected to be fundamental research
- Understand and comply with SAM, E-verify, FAPIIS, i-Edison and WAWF. Links are found in the BAA.
- For planning purposes - anticipated Program Start Date is April 1, 2016
- Subcontracting Issues
  - Non-Small Businesses: Subcontracting Plans required for FAR-based contracts expected to exceed the applicable threshold.
  - Subcontractor cost - Proposals must include, at a minimum, a non-proprietary, subcontractor proposal for EACH subcontractor.
  - If utilizing FFRDC, Government entity, or a foreign-owned firm as a subcontractor, submit their required eligibility information, as applicable.

ITEMS TO NOTE CONTINUED

- Proposals must be valid for a minimum of 120 days
- If a prospective proposer believes a conflict of interest exists or has a question on what constitutes a conflict - promptly raise the issue with DARPA
- Document files must be in .pdf, .odx, .doc, .docx, .xls, and/or .xlsx formats.
- Submissions must be written in English.

PROPOSAL SUBMISSION

- TA 1 submissions will be completely UNCLASSIFIED with the exception of Appendix C. Appendix C must be received before the BAA proposal submission dead line.
- Follow submission procedures outlined in the BAA. DO NOT submit proposals except as outlined in the BAA (e.g., email/fax submissions will NOT be accepted).
- Use DARPA's web-based upload system for unclassified portion of proposal. Submission must be in a single zip file not exceeding 50 MB.
- DO NOT include any classified information in the unclassified portion of the proposal or it may be deemed non conforming.
- DO NOT wait until the last minute to submit proposals – the submission deadlines as outlined in the BAA will be strictly enforced

EVALUATION / AWARD

- No common Statement of Work - Proposal evaluated on individual merit and relevance as it relates to the stated research goals/objectives

- Evaluation Criteria (listed in descending order of importance) are: (a) Overall Scientific and Technical Merit; (b) Potential Contribution and Relevance to the DARPA Mission; and (c) Cost Realism.

- Evaluation done by scientific/technical review process. DARPA SETAs with NDAs may assist in process.

- Government reserves the right to select for award all, some, or none of the proposals received, to award portions of a proposal, and to award with or without discussions.

COMMUNICATION

- Prior to Receipt of Proposals – No restrictions, however Gov't (PM/PCO) shall not dictate solutions or transfer technology. Unclassified FAQs will be periodically posted to this BAA's DARPA web page.

- After Receipt of Proposals – Prior to Selection: Limited to PCO – typical communication to address proposal clarifications.

- After Selection/Prior to Award: Communications range from technical clarifications/revisions to formal cost negotiations. May involve technical as well as contracting staff.

- Informal feedback for proposals not selected for funding may be provided once the selection(s), if any, are made.

Only a duly authorized Contracting Officer may obligate the Government

TAKE AWAY

- Submit proposals before the due date/time - Do NOT wait until the last minute to submit.
- Read and understand the BAA - Follow the BAA when preparing proposals.
- Be familiar with Government IP terms from the DFARS Part 227.
- Submit working/unprotected spreadsheet(s).
- The Contracting Officer is the only Government official authorized to obligate the Government.